The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

TLP: WHITE
Disclosure is not limited. Subject to standard copyright rules, TLP: WHITE information may be distributed without restriction.
http://www.us-cert.gov/tlp/

DATE(S) ISSUED:
03/09/2017

SUBJECT:
Vulnerability in Apache Struts Could Allow for Remote Code Execution

OVERVIEW:
A vulnerability has been discovered for Apache Software Foundation Struts version 2. Apache Struts is an open source framework used for building Java web applications. Successful exploitation of this vulnerability could allow for remote code execution in the context of the affected application. Depending on the privileges associated with the application, an attacker could install programs; view, change, or delete data; or create new accounts with full user rights.

THREAT INTELLIGENCE:
There are reports of this vulnerability being actively exploited in the wild. Exploit code is available.

SYSTEMS AFFECTED:
- Apache Struts versions 2.3.5 - 2.3.31, 2.5 to 2.5.10

RISK:
Government:
- Large and medium government entities: **High**
- Small government entities: **Medium**

Businesses:
- Large and medium business entities: **High**
- Small business entities: **Medium**

Home users: N/A

TECHNICAL SUMMARY
A vulnerability has been discovered in Apache Struts which could allow for remote code execution. An attacker can exploit this issue by sending a malicious Content-Type value as part of a file upload request on Struts installations configured to use the Jakarta Multipart parser (CVE-2017-5638), the default Multipart parser for Struts 2. If the Content-Type value is not valid, an exception occurs and an error message is displayed.

Successful exploitation of this vulnerability could allow for remote code execution in the context of the application. Depending on the privileges associated with the application, an attacker could install programs; view, change, or delete data; or create new accounts with full user rights.

RECOMMENDATIONS:
The following actions should be taken:

- Upgrade to one of the non-impacted versions of Adobe Struts (2.3.32 or 2.5.10.1), or follow the mitigation identified in the referenced Apache resources below after appropriate testing.
- Verify no unauthorized system modifications have occurred on system before applying the patch.
- Frequently validate type and content of uploaded data.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.

REFERENCES:
Apache:
https://cwiki.apache.org/confluence/display/WW/S2-045

CVE:
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5638

GitHub:
https://github.com/rapid7/metasploit-framework/issues/8064